2131
IFW

CERTIFICATE OF MAILING under 37 CFR 1.8

I herby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

on: April 12, 2006.

4/12/06

Sujata Barot

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Valdes, et al.	Attorney Docket No.:	10454-014002 (SRI/4190-3)
Serial No.:	09/711,323	Filed:	November 9, 2000
Examiner:	Aravind K. Moorthy	Group Art Unit:	2131

Title: SENSOR AND ALERT CORRELATION IN INTRUSION DETECTION SYSTEMS

COMMISSIONER FOR PATENTS
Mail Stop AF
PO Box 1450
Alexandria, VA 22313-1450

SIR:

Disclosure Statement under 37 C.F.R. §§ 1.56 and 1.98

Pursuant to 37 CFR § 1.56 and MPEP § 2001.06(c), the documents listed on the attached form PTO-1449 are disclosed.

Pursuant to 37 CFR § 1.98(a), the documents listed on the attached form PTO-1449 are submitted herewith. The Information Disclosure Statement submitted herewith is being filed after the period specified in 37 CFR 1.97(c), but on or before payment of the issue fee and is accompanied by the statement and fee as indicated below. The Commissioner is hereby authorized to charge counsel's Deposit Account No. 20-0782/SRI/4190-3 for the fee set forth in 37 CFR 1.17(p), as well as any other fees required to make this response timely and acceptable to the Office.

The documents listed on the attached form PTO-1449 comprise the responses to contention interrogatories made in the action captioned *SRI International Inc.* v.

04/20/2006 SDENBOB1 00000027 200782 09711323
01 FC:1806 180.00 DA

Internet Security Systems et al. currently pending in the U.S. District Court for the District of Delaware, case number 04-1199-SLR. The interrogatories relate to the defendants' allegations of inequitable conduct and to the validity of U.S. Patents 6,711,615, 6,484,203, 6,321,338, and 6,708,212.

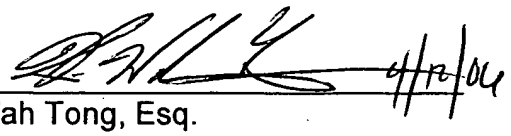
The documents listed as C1 through C51 on the attached form PTO-1449 are the defendants' interrogatory responses and exhibits thereto. The documents listed as C52 through C55 are the plaintiff's (Applicants') responses, including a rebuttal of the defendants' allegations of invalidity. The remainder of the documents provided herewith represent the art referenced in the defendants' responses that is not already of record in the present Application.

The final exhibit of each defendant's responses (*i.e.*, documents C25 and C49) alleges that the combination of an exceptionally large number of documents renders the patents in suit obvious. In order to avoid overly burdening the Examiner with this large volume of additional material, the Applicants have not provided copies of these references unless they are referenced elsewhere in the exhibits, or already of record in the present Application. However, the Applicants' representative will be more than happy to provide any or all of these references if the Examiner believes it necessary.

The Examiner's attention is directed to the fact that certain portions of the documents submitted herewith (particularly, certain portions of the defendant's invalidity contentions) are marked as subject to a protective order. The portions of the documents so marked include citations from an unpublished, internal and confidential document authored by the Applicants entitled "*Conceptual Design and Planning for EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances*" dated 20 May, 1997. This document has never been published or made available to the public, and as such cannot be prior art or otherwise material to patentability, and is not cited on the attached form PTO-1449. The Applicants do not object to the inclusion of the cited portions of this document, as recited in the defendant's invalidity contentions, in the official file wrapper maintained by the Office.

Further, two documents referenced by the defendants in their contentions are marked as "For Official Use Only": (i) "*Netranger Realtime Network Intrusion Detection Performance and Security Test*", DoD/SPOCK including appendices A, B, and C, April 30 1997 and (ii) "*Product Security Assessment of the Netranger Intrusion Detection Management System Version 1.1*", Air Force Information Warfare Center, February 1997. The Applicants are investigating the validity of these government markings and are unable at present to provide the Examiner with copies thereof. If it is determined that these markings are no longer appropriate, the Applicants will provide copies to the Examiner.

Respectfully submitted,



Kin-Wah Tong, Esq.
Registration No. 39,400
PATTERSON & SHERIDAN, LLP
595 Shrewsbury Avenue, Suite 100
Shrewsbury, NJ 07702
Telephone: (732) 530-9404
Facsimile: (732) 530-9808
Attorney for Applicants

PTO/SB/17 (12-04v2)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

OIPE IAP45 APR 20 2006 PATENT & TRADEMARK OFFICE

Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL for FY 2006

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT	($180.00)

Complete if Known	
Application Number	09/711,323
Filing Date	11/9/2000
First Named Inventor	VALDES, et al.
Examiner Name	Aravind K. Moorthy
Art Unit	2131
Attorney Docket No.	10454-014002 (SRI/4190-3)

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify) : _____

☒ Deposit Account Deposit Account Number: 20-0782 Deposit Account Name: Patterson & Sheridan, LLP.

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☒ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☒ Charge any additional fee(s) or underpayments of fee(s) Under 37 CFR 1.16 and 1.17 ☒ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
		Small Entity		Small Entity		Small Entity	
Application Type	Fee ($)	Fee($)	Fee($)	Fee($)	Fee($)	Fee($)	Fees Paid ($)
Utility	300	150	500	250	200	100	____
Design	200	100	100	50	130	65	____
Plant	200	100	300	150	160	80	____
Reissue	300	150	500	250	600	300	____
Provisional	200	100	0	0	0	0	____

2. EXCESS CLAIM FEES

Fee Description		Small Entity
	Fee ($)	Fee ($)
Each claim over 20 (including Reissues)	50	25
Each independent claim over 3 (including Reissues)	200	100
Multiple dependent claims	360	180

Total Claims	Extra Claims	Fee($)	Fee Paid ($)
____ -20 or HP=	____	x ____	= ____

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims	Extra Claims	Fee($)	Fee Paid ($)
____ - 3 or HP=	____	x ____	= ____

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims	
Fee ($)	Fee Paid ($)
____	____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof	Fee ($)	Fee Paid ($)
____ - 100 =	____	/ 50 = ____ (round up to a whole number) x		= ____

4. OTHER FEE(S)

	Fees Paid ($)
Non-English Specification, $130 fee (no small entity discount)	____
Other (e.g., late filing surcharge) : IDS	180.00

SUBMITTED BY

Signature	Diana J. Rea	Registration No. (Attorney/Agent)	54,938	Telephone	(723) 530-9404
Name (Print/Type)	Diana J. Rea, Esq.			Date	4/12/06

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing this form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Please type a plus sign (+) inside this box → [+]

CIPE IAP43 APR 20 2006 PATENT & TRADEMARK OFFICE

PTO/SB/08a (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 15

Application Number	09/711,323
Filing Date	11/9/2000
First Named Inventor	Valdes, et al.
Group Art Unit	2131
Examiner Name	Aravind K. Moorthy
Attorney Docket Number	10454-014002 (SRI/4190-3)
Submission Date	April 12, 2006

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1	US - 5,825,750	10-20-1998	Thompson	
	A2				
	A3				
	A4				
	A5				
	A6				
	A7				
	A8				
	A9				
	A10				
	A11				
	A12				
	A13				
	A14				
	A15				
	A16				
	A17				
	A18				

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
	B1					
	B2					
	B3					
	B4					
	B5					

Examiner Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.** *If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.*

Please type a plus sign (+) inside this box [+]

PTO/SB/08b (08-03)
Approved for use through 06/30/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

OIPE
APR 20 2006
PATENT & TRADEMARK OFFICE

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 | | 15

Application Number	09/711,323
Filing Date	11/9/2000
First Named Inventor	Valdes, et al.
Group Art Unit	2131
Examiner Name	Aravind K. Moorthy
Attorney Docket Number	10454-014002 (SRI/4190-3)
Submission Date	April 12, 2006

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C1	JOINT CLAIM CONSTRUCTION STATEMENT, SRI International, Inc., a California Corporation v. Internet Security Systems, Inc., a Delaware Corporation, Internet Security Systems, Inc., a Georgia Corporation, and Symantec Corporation a Delaware Corporation, (13 pages), Certificate of Service dated March 17, 2006	
	C2	SYMANTEC CORPORATION'S SECOND SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORIES NOS. 6 AND 11, SRI International, Inc., a California Corporation v. Internet Security Systems, Inc., a Delaware Corporation, Internet Security Systems, Inc., a Georgia Corporation and Symantec Corporation, a Delaware Corporation, pp 1-22, Dated November 15, 2005	
	C3	EXHIBIT A-1 TO THE SYMANTEC CORPORATION'S SECOND SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORIES NOS. 6 AND 11, EMERALD: EVENT MONITORING ENABLING RESPONSES TO ANOMALOUS LIVE DISTURBANCES, "EMERALD 1997", EMERALD 1997 INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b), pp. 1-51, November 15, 2005.	
	C4	EXHIBIT A-2 TO THE SYMANTEC CORPORATION'S SECOND SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORIES NOS. 6 AND 11, ANALYSIS AND RESPONSE FOR INTRUSION DETECTION IN LARGE NETWORKS- SUMMARY FOR CMAD WORKSHOP, "EMERALD-CMAD", EMERALD – CMAD INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b) AND/OR 103, pp.1-33, November 15, 2005.	
	C5	EXHIBIT A-3 TO THE SYMANTEC CORPORATION'S SECOND SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORIES NOS. 6 AND 11, EMERALD: EVENT MONITORING ENABLING RESPONSES TO ANOMALOUS LIVE DISTURBANCES CONCEPTUAL OVERVIEW, "EMERALD-CONCEPTUAL OVERVIEW", EMERALD – CONCEPUTAL OVERVIEW INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b) AND/OR 103, pp.1-34, November 15, 2005.	
	C6	EXHIBIT A-4 TO THE SYMANTEC CORPORATION'S SECOND SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORIES NOS. 6 AND 11, CONCEPTUAL DESIGN AND PLANNING FOR EMERALD: EVENT MONITORING ENABLING RESPONSES TO LIVE DISTURBANCES, "EMERALD – CONCEPTUAL DESIGN 1997", EMERALD – CONCEPTUAL DESIGN 1997 INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b) AND/OR 103 pp.1-56, November 15, 2005.	
	C7	EXHIBIT A-5 TO THE SYMANTEC CORPORATION'S SECOND SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORIES NOS. 6 AND 11, LIVE TRAFFIC ANALYSIS OF TCP/IP GATEWAYS, "EMERALD – LIVE TRAFFIC ANALYSIS", EMERALD – LIVE TRAFFIC ANALYSIS INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b), pp.1-44, November 15, 2004.	
	C8	EXHIBIT A-6 TO THE SYMANTEC CORPORATION'S SECOND SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORIES NOS. 6 AND 11, NEXT GENERATION INTRUSION DETECTION EXPERT SYSTEM (NIDES) A SUMMARY, "NETWORK NIDES", NETWORK NIDES INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b), pp.1-40, November 15, 2005	
	C9	EXHIBIT A-7 TO THE SYMANTEC CORPORATION'S SECOND SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORIES NOS. 6 AND 11, SCALABLE INTRUSION DETECTION FOR THE EMERGING NETWORK, "JI-NAO", EACH OF JI-NAO AND JI-NAO SLIDES INVALIDATE THE INDICATED CLAIMS UNDER 5 U.S.C. § 102 (b), pp.1-76, November 15, 2005.	

Examiner Date Considered

[1]EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.** *If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.*

Please type a plus sign (+) inside this box → [+]

OIPE IAP43
APR 20 2006
PATENT & TRADEMARK OFFICE

PTO/SB/08b (08-03)
Approved for use through 06/30/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 3 | 15

Application Number	09/711,323
Filing Date	11/9/2000
First Named Inventor	Valdes, et al.
Group Art Unit	2131
Examiner Name	Aravind K. Moorthy
Attorney Docket Number	10454-014002 (SRI/4190-3)
Submission Date	April 12, 2006

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C10	EXHIBIT A-8 TO THE SYMANTEC CORPORATION'S SECOND SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORIES NOS. 6 AND 11, A NETWORK SECURITY MONITOR, "NSM", NSM INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b), pp. 1-9, November 15, 2005.	
	C11	EXHIBIT A-9 TO THE SYMANTEC CORPORATION'S SECOND SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORIES NOS. 6 AND 11, DISTRIBUTED INTRUSION DETECTION SYSTEM, "DIDS FEBRUARY 1991 AND DIDS OCTOBER 1991", EACH OF DIDS FEBRUARY 1991 AND DIDS OCTOBER 1991 INVALIDATE THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b), pp. 1-88, November 15, 2005.	
	C12	EXHIBIT A-10 TO THE SYMANTEC CORPORATION'S SECOND SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORIES NOS. 6 AND 11, GRAPH BASED INTRUSION DETECTION SYSTEM FOR LARGE NETWORKS, "GRIDS 1996 AND GRIDS 1997", GRIDS 1996 AND GRIDS 1997 INVALIDATE THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b), pp. 1-39, November 15, 2005.	
	C13	EXHIBIT A-11 TO THE SYMANTEC CORPORATION'S SECOND SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORIES NOS. 6 AND 11, WHEELGROUP CORPORATION, "NETRANGER", EACH OF NETRANGER USER GUIDE 1.3.1 INVALIDATE THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b), pp. 1-34, November 15, 2005.	
	C14	EXHIBIT A-12 TO THE SYMANTEC CORPORATION'S SECOND SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORIES NOS. 6 AND 11, INTERNET SECURITY SYSTEMS, "REALSECURE", REALSECURE INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b), pp.1-22, November 15, 2005.	
	C15	EXHIBIT A-13 TO THE SYMANTEC CORPORATION'S SECOND SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORIES NOS. 6 AND 11, THE ARCHITECTURE OF A NETWORK LEVEL INTRUSION DETECTION SYSTEM, "NETWORK LEVEL INTRUSION DETECTION", NETWORK LEVEL INTRUSION DETECTION INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b), pp. 1-20, November 15, 200.	
	C16	EXHIBIT A-14 TO THE SYMANTEC CORPORATION'S SECOND SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORIES NOS. 6 AND 11, U.S. PATENT NO. 5,825,750 (THOMPSON), U.S. PAT. NO. 5,825,750 (THOMPSON) INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (a) AND 102(e), pp.1-13, November 15, 2005.	
	C17	EXHIBIT A-15 TO THE SYMANTEC CORPORATION'S SECOND SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORIES NOS. 6 AND 11, FAULT DETECTION IN AN ETHERNET NETWORK VIA ANOMALY DETECTORS, FAULT DETECTION IN AN ETHERNET NETWORK VIA ANOMALY DETECTORS INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b), pp.1-9, November 15, 2005.	

Examiner Date Considered

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.** *If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.*

Please type a plus sign (+) inside this box → [+]

PTO/SB/08b (08-03)
Approved for use through 06/30/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

IAP20 APR 20 2006 PATENT & TRADEMARK OFFICE

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	4		15

Application Number	09/711,323
Filing Date	11/9/2000
First Named Inventor	Valdes, et al.
Group Art Unit	2131
Examiner Name	Aravind K. Moorthy
Attorney Docket Number	10454-014002 (SRI/4190-3)
Submission Date	April 12, 2006

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C18	EXHIBIT A-16 TO THE SYMANTEC CORPORATION'S SECOND SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORIES NOS. 6 AND 11, HARRIS CORPORATION, "STAKE OUT NETWORK SURVEILLANCE", STAKE OUT NETWORK SURVEILLANCE INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b), pp.1-12, November 15, 2005.	
	C19	EXHIBIT A-17 TO THE SYMANTEC CORPORATION'S SECOND SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORIES NOS. 6 AND 11, HP OPENVIEW FOR WINDOWS USER GUIDE, "HP OPENVIEW", HP OPENVIEW AND THE INTERNET STANDARDS INVALIDATE THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b) AND/OR 103, pp.1-29, November 15, 2005.	
	C20	EXHIBIT A-18 TO THE SYMANTEC CORPORATION'S SECOND SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORIES NOS. 6 AND 11, INTERNETWORK SECURITY MONITOR, "ISM", ISM AND DIDS INVALIDATE THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b) OR 103, pp. 1-80, November 15, 2005.	
	C21	EXHIBIT A-19 TO THE SYMANTEC CORPORATION'S SECOND SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORIES NOS. 6 AND 11, EMERALD 1997, INTRUSIVE ACTIVITY 1991, NIDES 1994, EMERALD 1997, INTRUSIVE ACTIVITY 1991, AND NIDES 1994 INVALIDATE THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b) AND/OR 103, pp. 1-53, November 15, 2005.	
	C22	EXHIBIT A-20 TO THE SYMANTEC CORPORATION'S SECOND SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORIES NOS. 6 AND 11, NETSTALKER AND HP OPENVIEW, NETSTALKER AND HP OPENVIEW INVALIDATE THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b) AND/OR 103, pp.1-32, November 15, 2005.	
	C23	EXHIBIT A-21 TO THE SYMANTEC CORPORATION'S SECOND SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORIES NOS. 6 AND 11,NETWORK FLIGHT RECORDER, NETWORK FLIGHT RECORDER INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b) AND/OR 103, pp. 1-53, November 15, 2005.	
	C24	EXHIBIT A-22 TO THE SYMANTEC CORPORATION'S SECOND SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORIES NOS. 6 AND 11, AUTOMATED INFORMATION SYSTEM "AIS", AIS INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b), pp. 1-21, November 15, 2005.	
	C25	EXHIBIT A-23 TO THE SYMANTEC CORPORATION'S SECOND SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORIES NOS. 6 AND 11, COMPARISON OF LISTED PUBLICATIONS TO CLAIMS –AT-ISSUE OF SRI'S PATENT-IN-SUIT FOR 35 U.S.C. § 103, pp. 1-57, November 15, 2005.	

Examiner Date Considered

[1]EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.** *If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.*

Please type a plus sign (+) inside this box → [+]

PTO/SB/08b (08-03)
Approved for use through 06/30/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 5 | 15

Application Number	09/711,323
Filing Date	11/9/2000
First Named Inventor	Valdes, et al.
Group Art Unit	2131
Examiner Name	Aravind K. Moorthy
Attorney Docket Number	10454-014002 (SRI/4190-3)
Submission Date	April 12, 2006

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C26	SUPPLEMENTAL RESPONSES AND OBJECTIONS OF ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NOS 6 & 11, SRI International, Inc., a California Corporation v. Internet Security Systems Inc., a Delaware Corporation, Internet Security Systems, Inc., a Georgia Corporation, and Symantec Corporation, a Delaware Corporation, pp.1-22, Certificate of Service dated November 15, 2005	
	C27	EXHIBIT 1 TO THE SUPPLEMENTAL RESPONSES AND OBJECTIONS OF ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NOS 6 & 11, EMERALD 1997 INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b), pp.1-60, November 15, 2005.	
	C28	EXHIBIT 2 TO THE SUPPLEMENTAL RESPONSES AND OBJECTIONS OF ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NOS 6 & 11, CMAD INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b) AND/OR 103,pp 1-27, November 15, 2005.	
	C29	EXHIBIT 3 TO THE SUPPLEMENTAL RESPONSES AND OBJECTIONS OF ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NOS 6 & 11, EMERALD CONCEPTUAL OVERVIEW INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C.§ 102 (b) AND/OR 103, pp. 1-35, November 15, 2005.	
	C30	EXHIBIT 4 TO THE SUPPLEMENTAL RESPONSES AND OBJECTIONS OF ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NOS 6 & 11, CONCEPTUAL DESIGN AND PLANNING FOR EMERALD: EVENT MONITORING ENABLING RESPONSES TO ANOMALOUS LIVE DISTURBANCES VERSION 1.2, 20 May 1997INVALIDATE THE INDICATED CLAIMS UNDER 35 U.S.C.§ 102 (b) AND/OR 103, pp. 1-58, November 15, 2005.	
	C31	EXHIBIT 5 TO THE SUPPLEMENTAL RESPONSES AND OBJECTIONS OF ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NOS 6 & 11, LIVE TRAFFIC ANALYSIS INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C.§ 102 (b), PP. 1-52, November 15, 2005.	
	C32	EXHIBIT 6 TO THE SUPPLEMENTAL RESPONSES AND OBJECTIONS OF ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NOS 6 & 11, NEXT-GENERATION INTRUSION DETECTION EXPERT SYSTEM (NIDES): A SUMMARY INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C.§ 102 (b), pp. 1-47, November 15, 2005	
	C33	EXHIBIT 7 TO THE SUPPLEMENTAL RESPONSES AND OBJECTIONS OF ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NOS 6 & 11, JI-NAO INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C.§ 102 (b), pp.1-100, November 15, 2005	

Examiner Date Considered

[1]EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [2] Applicant's unique citation designation number (optional). [3] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.** *If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.*

Please type a plus sign (+) inside this box → [+]

OIPE
APR 20 2006
PATENT & TRADEMARK OFFICE

PTO/SB/08b (08-03)
Approved for use through 06/30/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 6 | 15

Application Number	09/711,323
Filing Date	11/9/2000
First Named Inventor	Valdes, et al.
Group Art Unit	2131
Examiner Name	Aravind K. Moorthy
Attorney Docket Number	10454-014002 (SRI/4190-3)
Submission Date	April 12, 2006

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C34	EXHIBIT 8 TO THE SUPPLEMENTAL RESPONSES AND OBJECTIONS OF ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NOS 6 & 11, NSM INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C.§ 102 (b), pp.1-17, November 15, 2005.	
	C35	EXHIBIT 9 TO THE SUPPLEMENTAL RESPONSES AND OBJECTIONS OF ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NOS 6 & 11, DIDS INVALIDATES THE INDICATED CLIAMS UNDER 35 U.S.C.§ 102 (b), pp.1-114, November 15, 2005.	
	C36	EXHIBIT 10 TO THE SUPPLEMENTAL RESPONSES AND OBJECTIONS OF ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NOS 6 & 11, ISM AND DIDS INVALIDATE THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b) OR 103. pp.1-91, November 15, 2005.	
	C37	EXHIBIT 11 TO THE SUPPLEMENTAL RESPONSES AND OBJECTIONS OF ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NOS 6 & 11, GrIDS INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C.§ 102 (b), pp.1-41, November 15, 2005	
	C38	EXHIBIT 12 TO THE SUPPLEMENTAL RESPONSES AND OBJECTIONS OF ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NOS 6 & 11, NETRANGER INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C.§ 102 (b), pp,1-32, November 15, 2005.	
	C39	EXHIBIT 13 TO THE SUPPLEMENTAL RESPONSES AND OBJECTIONS OF ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NOS 6 & 11, REALSECURE INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C.§ 102 (b), pp. 1-21, November 15, 2005.	
	C40	EXHIBIT 14 TO THE SUPPLEMENTAL RESPONSES AND OBJECTIONS OF ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NOS 6 & 11, THE NETWORK FLIGHT RECORDER SYSTEM INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b) AND/OR 103, pp.1-73, November 15, 2005.	
	C41	EXHIBIT 15 TO THE SUPPLEMENTAL RESPONSES AND OBJECTIONS OF ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NOS 6 & 11, NETSTALKER AND HP OPENVIEW INVALIDATE THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b) AND/OR 103, pp.1-21, November 15, 2005.	

Examiner | Date Considered

'EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.** *If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.*

Please type a plus sign (+) inside this box → [+]

OIPE APR 20 2006 PATENT & TRADEMARK OFFICE

PTO/SB/08b (08-03)
Approved for use through 06/30/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 7 | | 15

Application Number	09/711,323
Filing Date	11/9/2000
First Named Inventor	Valdes, et al.
Group Art Unit	2131
Examiner Name	Aravind K. Moorthy
Attorney Docket Number	10454-014002 (SRI/4190-3)
Submission Date	April 12, 2006

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C42	EXHIBIT 16 TO THE SUPPLEMENTAL RESPONSES AND OBJECTIONS OF ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NOS 6 & 11, HP OPENVIEW AND THE INTERNET STANDARDS INVALIDATE THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b) AND/OR 103, pp.1-26, November 15, 2005.	
	C43	EXHIBIT 17 TO THE SUPPLEMENTAL RESPONSES AND OBJECTIONS OF ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NOS 6 & 11," NETWORK LEVEL INTRUSION DETECTION SYSTEM" (AUGUST 1990) INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b), pp.1-22, November 15, 2005.	
	C44	EXHIBIT 18 TO THE SUPPLEMENTAL RESPONSES AND OBJECTIONS OF ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NOS 6 & 11, US PATENT NUMBER 5,825,750 (THOMPSON) INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (a) and 102 (e), pp.1-21, November 15, 2005.	
	C45	EXHIBIT 19 TO THE SUPPLEMENTAL RESPONSES AND OBJECTIONS OF ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NOS 6 & 11," FAULT DETECTION IN AN ETHERNET NETWORK VIA ANOMALY DETECTORS" INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b), pp. 1-17, November 15, 2005.	
	C46	EXHIBIT 20 TO THE SUPPLEMENTAL RESPONSES AND OBJECTIONS OF ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NOS 6 & 11, STAKE OUT NETWORK SURVEILLANCE INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b), pp.1-24, November 15, 2005.	
	C47	EXHIBIT 21 TO THE SUPPLEMENTAL RESPONSES AND OBJECTIONS OF ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NOS 6 & 11, EMERALD 1997, INTRUSIVE ACTIVITY 1991, AND NIDES 1994 INVALIDATE THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b) OR 103,pp. 1-62, November 15, 2005.	
	C48	EXHIBIT 22 TO THE SUPPLEMENTAL RESPONSES AND OBJECTIONS OF ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NOS 6 & 11, AUTOMATED INFORMATION SYSTEM – AIS INVALIDATES THE INDICATED CLAIMS UNDER 35 U.S.C. § 102 (b), pp. 1-15, November 15, 2005.	
	C49	EXHIBIT 23 TO THE SUPPLEMENTAL RESPONSES AND OBJECTIONS OF ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NOS 6 & 11, COMPARISON OF LISTED PUBLICATIONS TO CLAIMS-AT-ISSUE OF SRI'S PATENTS-IN-SUIT FOR 35 U.S.C. § 103, pp. 1-127, November 15, 2005.	
	C50	SECOND SUPPLEMENTAL RESPONSES AND OBJECTIONS OF ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NO. 11,SRI International, Inc., a California Corporation v. Internet Security Systems, Inc., a Delaware Corporation, Internet Security Systems, Inc., a Georgia Corporation and Symantec Corporation a Delaware Corporation, pp.1-17, Certificate of Service dated March 28, 2006.	
	C51	SYMANTEC CORPORATION'S FIFTH SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORY NO. 11, SRI International, Inc., a California Corporation v. Internet Security Systems, Inc., a Delaware Corporation, Internet Security Systems, Inc., a Georgia Corporation and Symantec Corporation a Delaware Corporation, pp. 1-15, dated March 28, 2006.	
	C52	SRI INTERNATIONAL, INC.'S RESPONSES TO DEFENDANTS ISS-GA'S SECOND SET OF INTEROGATORIES (NOS. 19-20) AND SRI'S THIRD SUPPLEMENTAL RESPONSE TO ISS-GA'S INTERROGATORY NO. 17, SRI International, Inc., a California Corporation v. Internet Security Systems, Inc., a Delaware Corporation, Internet Security Systems, Inc., a Georgia Corporation and Symantec Corporation a Delaware Corporation, pp. 1-54, Certificate of Service dated December 15, 2005	

Examiner Date Considered

'EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.** *If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.*

Please type a plus sign (+) inside this box → [+]

OIPE IAP
APR 20 2006
PATENT AND TRADEMARK OFFICE

PTO/SB/08b (08-03)
Approved for use through 06/30/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 8 | 15

Application Number	09/711,323
Filing Date	11/9/2000
First Named Inventor	Valdes, et al.
Group Art Unit	2131
Examiner Name	Aravind K. Moorthy
Attorney Docket Number	10454-014002 (SRI/4190-3)
Submission Date	April 12, 2006

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C53	SRI INTERNATIONAL, INC.'S RESPONSE TO SYMANTEC'S INVALIDITY AND INEQUITABLE CONDUCT CONTENTIONS, SRI International, Inc., a California Corporation v. Internet Security Systems, Inc., a Delaware Corporation, Internet Security Systems, Inc., a Georgia Corporation and Symantec Corporation a Delaware Corporation, pp.1-50, Certificate of Service dated December 15, 2005	
	C54	SRI INTERNATIONAL, INC.'S SUPPLEMENTAL RESPONSE TO INTERROGATORIES NO 12. AND NO. 15, SRI International, Inc., a California Corporation v. Internet Security Systems, Inc. a Delaware Corporation, Internet Security Systems, Inc. a Georgia Corporation and Symantec Corporation a Delaware Corporation, pp. 1-6, Certificate of Service date December 15, 2005	
	C55	SRI INTERNATIONAL, INC.'S "AMENDED" RESPONSE TO SYMANTEC'S INVALIDITY AND INEQUITABLE CONDUCT CONTENTIONS, SRI International, Inc., a California Corporation v. Internet Security Systems, Inc., a Delaware Corporation, Internet Security Systems, Inc., a Georgia Corporation and Symantec Corporation a Delaware Corporation, pp.1-51, Certificate of Service date December 16, 2005	
	C56	S.S. CHEN et al, GrIDS – A Graph Based Intrusion Detection System for Large Networks, 19th National Information Security Systems Conference, 1996	
	C57	L.T. HEBERLEIN, et al., Internetwork Security Monitor, Proc. 15th National Computer Security Conference, October 13-16 1992, pp. 262-271	
	C58	B. MUKHERJEE et al., Network Intrusion Detection, IEEE Network 8(3), pp. 26-41, May/June 1994	
	C59	B. GLEICHAUF AND D. TEAL, NetRanger High-level Overview Version 1.1, WheelGroup Corp., November 1996	
	C60	S.R. SNAPP, et al., A System for Distributed Intrusion Detection, COMPCON Spring'91, Digest of Papers, San Francisco, CA, 25 February – 1 March 1991, pp. 170-176	
	C61	JAMES BRENTANO et al., An Architecture for a Distributed Intrusion Detection System, Proc. 14th Department of Energy Computer Security Group Conference, May 7-9 1991, pp 17.25-17.45.	
	C62	L.T. HEBERLEIN et al., Towards Detecting Intrusions in a Networked Environment, Proc. 14th Department of Energy Computer Security Group Conference, pp. 17.47-17.65, May 7-9 1991	

Examiner Date Considered

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.** *If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.*

OIPE IAP43 APR 20 2006 PATENT & TRADEMARK OFFICE

Please type a plus sign (+) inside this box → +

PTO/SB/08b (08-03)
Approved for use through 06/30/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	9		15

Application Number	09/711,323
Filing Date	11/9/2000
First Named Inventor	Valdes, et al.
Group Art Unit	2131
Examiner Name	Aravind K. Moorthy
Attorney Docket Number	10454-014002 (SRI/4190-3)
Submission Date	April 12, 2006

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C63	L.T. HEBERLEIN , Towards Detecting Intrusions in a Networked Environment, Technical Report CSE-91-23, Division of Computer Science, UC Davis, June 1991	
	C64	L.T. HEBERLEIN et al., A Method to Detect Intrusive Activity in a Networked Environment, Proc. 14th National Computer Security Conference, pp. 362-371, October 1991	
	C65	RANUM et al., Implementing a Generalized Tool for Network Monitoring, Proc. 11th Systems Administration Conference (LISA'97), San Diego, CA, October 1997	
	C66	STEVEN SNAPP et al., Intrusion Detection Systems (IDS): A Survey of Existing Systems and a Proposed Distributed IDS Architecture, CSE-91-7, allegedly dated February 1991	
	C67	L.T. HEBERLEIN et al., Network Attacks and an Ethernet-based Network Security Monitor, Proc. 13th Department of Energy Computer Security Group Conference, pp. 14.1-14.13, May 8-10 1990	
	C68	RealSecure 1.1: User Guide and Reference Manual, 1997	
	C69	RealSecure 1.2: User Guide and Reference Manual 1997	
	C70	3Com, HP Openview for Windows User Guide for Transcend Management Software, Version 6.1 for Windows and '97 for Windows NT, October 1997	
	C71	3Com, HP Openview for Windows Workgroup Node Manager User Guide for Transcend Management Software, Version 6.0 for Windows, January 1997	
	C72	Y. FRANK JOU et al., Architecture Design of a Scalable Intrusion Detection System For the Emerging Network Infrastructure, Technical Report CDRL A005, DARPA Order E296, Department of Computer Science, North Carolina State University, April 1997	
	C73	Y. FRANK JOU AND S. FELIX WU, Scalable Intrusion Detection for Emerging Network Infrastructures, IDS Program Review Presentation, SRI, July 1997	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.** *If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.*

Please type a plus sign (+) inside this box → [+]

OIPE IAP43
APR 20 2006
PATENT & TRADEMARK OFFICE

PTO/SB/08b (08-03)
Approved for use through 06/30/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	10		15

Application Number	09/711,323
Filing Date	11/9/2000
First Named Inventor	Valdes, et al.
Group Art Unit	2131
Examiner Name	Aravind K. Moorthy
Attorney Docket Number	10454-014002 (SRI/4190-3)
Submission Date	April 12, 2006

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C75	SHYHTSUN F. WU et al., Intrusion Detection for Link-state Routing Protocols, December 2, 1996	
	C76	DIHENG QU et al., Statistical Anomaly Detection for Link-state Routing Protocols, 6th International Conference on Network Protocol (ICNP '98), pp. 62-70, October 1998	
	C77	T. LUNT et al., A Real-time Intrusion Detection Expert System (IDES): Final Technical Report, Technical Report, SRI Computer Science Laboratory, Menlo Park, CA, 28 February 1992	
	C78	T.F. LUNT et al., IDES: A Progress Report, Proc. 6th Annual Computer Security Applications Conference, pp. 273-285, 1990	
	C79	PC Week, NetRanger Keeps Watch Over Security Leaks, September 1997	
	C80	Network Systems Corp., Data Privacy Facility Administrator's Guide Version 1.2, September 1995	
	C81	Haystack Labs, NetStalker, Installation and User's Guide, Version 1.0.2, 1996	
	C82	WheelGroup Corp., NetRanger User's Guide, 1996	
	C83	WheelGroup Corp., NetRanger User's Guide 1.2, 1997	
	C84	P.PORRAS AND P. NEUMANN, EMERALD : Event Monitoring Enabling Responses to Anomalous Live Disturbances Conceptual Overview, December 18, 1996	
	C85	WheelGroup Corp, WheelGroup Press Release Summary, undated.	
	C86	WheelGroup Corp., WheelGroup Releases NetRanger 2.0, Press Release, August 25, 1997	

Examiner Date Considered

[1]EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.** *If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.*

Please type a plus sign (+) inside this box → +

OIPE IAP43 APR 20 2006 PATENT & TRADEMARK OFFICE

PTO/SB/08b (08-03)
Approved for use through 06/30/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 11 | 15

Application Number	09/711,323
Filing Date	11/9/2000
First Named Inventor	Valdes, et al.
Group Art Unit	2131
Examiner Name	Aravind K. Moorthy
Attorney Docket Number	10454-014002 (SRI/4190-3)
Submission Date	April 12, 2006

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C87	WheelGroup Corp., Summary of DoD/SPOCK Evaluation of WheelGroup's NetRanger Intrusion Detection System, Press Release, July 8, 1997	
	C88	WheelGroup Corporation, NetRanger User Guide Version 1.3.1, 1997	
	C89	Graph-based Intrusion Detection System (GRIDS) Home Page, webpage allegedly archived July 19, 1997	
	C90	GrIDS Requirements Document, webpage allegedly archived December 14, 1996	
	C91	GrIDS Outline Design Document, webpage allegedly archived December 14, 1996	
	C92	STEVEN CHEUNG et al., The Design of GRIDS: A Graph-based Intrusion Detection System, Technical Report, UC Davis Department of Computer Science, May 14, 1997	
	C93	STEVEN CHEUNG et al., Graph-based Intrusion Detection System, Presentation at PI Meeting, Savannah, GA, Feb 25-27 1997	
	C94	WheelGroup Corp., NetRanger User's Guide 1.2.2, 1997	
	C95	R. POWER et al., Detecting Network Intruders, Network Magazine, pp. 137-38, October 1997	
	C96	P. NEUMANN, P. PORRAS AND A. VALDES, Analysis and Response for Intrusion Detection in Large Networks, Summary for CMAD Workshop, Monterey, 12-14 November 1996	
	C97	HP SNMP/XL User's Guide, HP 3000 MPE/iX Computer Systems Edition 5, Hewlett-Packard, April 1994	
	C98	M. SIEGL et al., Hierarchical Network Management – A Concept and its Prototype in SNMPv2, allegedly dated 1996	
	C99	RFC 1155, Structure and Identification of Management Information for TCP/IP-based Intranets, May 1990	

Examiner Date Considered

[1]EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.** *If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.*

Please type a plus sign (+) inside this box → [+]

OIPE IAP43
APR 20 2006
PATENT & TRADEMARK OFFICE

PTO/SB/08b (08-03)
Approved for use through 06/30/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	12		15

Application Number	09/711,323
Filing Date	11/9/2000
First Named Inventor	Valdes, et al.
Group Art Unit	2131
Examiner Name	Aravind K. Moorthy
Attorney Docket Number	10454-014002 (SRI/4190-3)
Submission Date	April 12, 2006

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C100	RFC 1157, A Simple Network Management Protocol (SNMP), May 1990	
	C101	RFC 1213, Management Information Base for Network Management of TCP/IP-based Internets: MIB-II, March 1991	
	C102	RFC 1441, Introduction to Version 2 of the Internet-standard Network Management Framework, April 1993	
	C103	RFC 1757, Remote Network Monitoring Management Information Base, February 1995	
	C104	RFC 1271, Remote Network Monitoring Management Information Base, November 1991	
	C105	RFC 1451, Manager-to-Manager Management Information Base, April 1993	
	C106	RICHARD HEADY et al., The Architecture of a Network Level Intrusion Detection System, Technical Report CS90-20, University of New Mexico, Department of Computer Science, August 15, 1990	
	C107	ISS, RealSecure 1.0: User Guide and Reference Manual, 1996	
	C108	KARL LEVITT AND CHRISTOPHER WEE (Eds.) Proceedings of Fourth Workshop on Future Directions in Computer Misuse and Anomaly Detection, Monterey, California, November 12-14 1996	
	C109	Netranger, Installation & Configuration Training, Slide Presentation, April 1997	
	C110	WheelGroup Corp., Traditional Security Basics, Undated	
	C111	T.F. LUNT et al., A Real-time Intrusion Detection Expert System (IDES): Interim Progress Report Project 6784, SRI International, May 1990	
	C112	ISS, RealSecure web page, allegedly dated 1997	

Examiner Date Considered

[1]EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.** *If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.*

Please type a plus sign (+) inside this box →

PATENT TRADEMARK OFFICE APR 20 2006 IAP43

PTO/SB/08b (08-03)
Approved for use through 06/30/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Application Number	09/711,323
Filing Date	11/9/2000
First Named Inventor	Valdes, et al.
Group Art Unit	2131
Examiner Name	Aravind K. Moorthy
Attorney Docket Number	10454-014002 (SRI/4190-3)
Submission Date	April 12, 2006

Sheet 13 | 15

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C113	ISS, Built-in Attack Recognition Capabilities Give Organizations Power to Detect and Respond to Attacks Before It's Too Late, Press release, May 12, 1997	
	C114	ISS, More About RealSecure: General Description and Comparison to Existing Systems, web page, allegedly available July 21, 1997	
	C115	ISS, Frequently Asked Questions about RealSecure, web page, allegedly last updated May 30th 1997, and alleged available July 21, 1997	
	C116	ISS,, Frequently Asked Questions about RealSecure, web page, allegedly last updated October 21st 1997, and alleged available January 20, 1998	
	C117	ISS, Frequently Asked Questions about RealSecure, web page, alleged available 1998	
	C118	ISS, Real-time Attack Recognition and Response: A Solution for Tightening Network Security, allegedly available January 20, 1998	
	C119	ISS, Internet Security Systems Launches RealSecure 1.0 For Windows NT, Press release, May 12, 1997	
	C120	ISS, Internet Security Systems Augments Network Security with Real-time Attack Recognition and Response Tool, Press release, December 9, 1996	
	C121	ISS, Internet Security Systems Ships RealSecure For Windows NT, Industry's First Real-time Attack Recognition and Response Tool for Windows NT, Press release, August 19, 1997	
	C122	ISS, ISS Announces New Version of Leading Real-time Security Attack Recognition and Response Tool, Press release, March 25, 1997	
	C123	Harris Corporation, Stake Out Network Surveillance, White Paper, 1996	
	C124	ISS, RealSecure Release Dates Table, Undated.	
	C125	MARK MILLER, Managing Internetworks with SNMP, 2nd Edition, 1997	
	C126	NFR, Frequently Asked Questions / Troubleshooting Guide, Undated	

Examiner Date Considered

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.** *If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.*

All GrIDS software is in the form of modules with a standardized interface. The modules are started, stopped, and controlled by a module controller process located on each host.

Each department has two special modules: the software manager and the graph engine. The software manager is responsible for managing the state of the hierarchy and the distributed modules. The hierarchy is re-arranged dynamically by drag-and-drop in a user interface, and starting and stopping particular modules is similarly automated.

GrIDS data sources are modules that monitor activity on hosts and networks and send reports of detected activity to the engine. The activity is reported in the form of a node or an edge for possible inclusion in an activity graph.

Data sources that are part of GrIDS include network sniffers and point IDSs (intrusion detection systems that work on a single host or LAN). However, GrIDS provides an extensible mechanism such that other security tools can be incorporated as data sources without significant change to the tool or GrIDS.

The graph engine takes input from data source modules. The engine builds graphs, and then passes summaries of those graphs up to the engine for its parent department. The parent engine, in turn, builds graphs which have a coarser resolution.

In addition to the components shown, there are user interface modules for allowing human interaction with the system, management functions, and display of alerts. There is also a central organizational hierarchy server which has a global view of the topology of the hierarchy, and is responsible for ensuring that changes to the hierarchy happen in a consistent manner.

2.3 Graph Building

This section discusses the GrIDS *engine*, which collects reports from the data sources and builds them into graphs.

Graphs consist of nodes and directed edges. A single graph represents a causally connected set of events on the network. Nodes represent hosts or departments, and edges represent network traffic between them. Nodes and edges are annotated with attributes that hold supplementary information. In addition, a graph has *global attributes* which maintain state information about the graph as a whole.

Because GrIDS searches for numerous types of network abuse, different kinds of graph are needed. Graphs are constructed in a flexible way; users write *rule sets* which specify how graphs are built from reports. A single graph containing all network activity is too awkward to analyze effectively, so GrIDS allows multiple rule sets. For each rule set it maintains a *graph space* which contains a number of connected graphs. A rule set is an executable specification of one kind of graph; it determines whether an incoming report will be incorporated into existing graphs, and what the results will be. It also specifies when the engine will consider a graph as suspicious and what actions to take if it is. Rule sets operate independently from one another.

Each new report is presented to each rule set in the form of a partial graph. If the report satisfies the rule set's *preconditions*, the engine considers adding the report to the graphs in that rule set's graph space.

A rule set specifies *combining rules* (for nodes and for edges), to determine if an incoming graph should be combined with an existing overlapping graph, and how that should occur. Disjoint graphs cannot be combined. If a combining condition is satisfied on at least one node or edge, then the incoming graph is combined with that existing graph, and the graph's attributes are recomputed. Finally, if no graph combining occurs, but the incoming report did pass the preconditions, then it forms a new graph in the graph space.

2.3.1 An Example Rule Set

Rule sets serve several purposes: to decide if two graphs should combine, to compute the attributes of the combined graph, and to decide what actions to take, if any. Computing the edges and nodes in the combined graph is a straightforward matter which the engine does automatically. However, since it does not know the semantics of user-defined attributes, the rule set must specify how to combine them

A rule set consists of several sections:

- A name
- Initializations
- Preconditions
- Graph combining rules
- Assessment and actions

GrIDS–A GRAPH BASED INTRUSION DETECTION SYSTEM FOR LARGE NETWORKS*

S. Staniford-Chen, S. Cheung, R. Crawford, M. Dilger,
J. Frank, J. Hoagland, K. Levitt, C. Wee, R. Yip, D. Zerkle

Department of Computer Science,
University of California, Davis,
Davis, CA 95616

email: <*lastname*>*@cs.ucdavis.edu*

Abstract

There is widespread concern that large-scale malicious attacks on computer networks could cause serious disruption to network services. We present the design of GrIDS (Graph-Based Intrusion Detection System). GrIDS collects data about activity on computers and network traffic between them. It aggregates this information into activity graphs which reveal the causal structure of network activity. This allows large-scale automated or co-ordinated attacks to be detected in near real-time. In addition, GrIDS allows network administrators to state policies specifying which users may use particular services of individual hosts or groups of hosts. By analyzing the characteristics of the activity graphs, GrIDS detects and reports violations of the stated policy. GrIDS uses a hierarchical reduction scheme for the graph construction, which allows it to scale to large networks. An early prototype of GrIDS has successfully detected a worm attack.

Keywords: Intrusion detection, networks, information warfare, computer security, graphs.

1 Introduction

The Internet is increasingly important as the vehicle for global electronic commerce. Many organizations also use Internet TCP/IP protocols to build intra-networks (intranets) to share and disseminate internal information. A large scale attack on these networks can cripple important world-wide Internet operations. The Internet Worm of 1988 caused the Internet to be unavailable for about five days [1]. Seven years later, there is no system to detect or analyze such a problem on an Internet-wide scale. The development of a secure infrastructure to defend the Internet and other networks is a major challenge.

In this paper, we present the design of the *Graph-based Intrusion Detection System* (GrIDS). GrIDS' design goal is to analyze network activity on TCP/IP networks with up to several thousand hosts. Its primary function is to detect and analyze large-scale attacks, although it also has the capability of detecting intrusions on individual hosts. GrIDS aggregates network activity of interest into *activity graphs*, which are evaluated and possibly reported to a system security officer (SSO). The hierarchical architecture of GrIDS allows it to scale to large networks.

GrIDS is being designed and built by the authors using formal consensus decision-making and a well-documented software process. We have completed the GrIDS design and have almost finished building a prototype.

This paper is organized as follows. Section 1.1 briefly describes related work on intrusion detection systems and motivates the need for GrIDS. Section 1.2 discusses classes of attacks that we expect to detect. In Section 2.1, the simple GrIDS detection algorithm is described, followed by a more detailed

*The work reported here is supported by DARPA under contract DOD/DABT 63-93-C-0045.

SYM_P_0068883